C8 con't

separating by the second member the first session key for each of the first members from the key exchange response message; and

sending each of the first session keys to its respective first member.

REMARKS

Claims 81-116 remain in this application. Claims 54-80 have been canceled without prejudice. Claims 81, 84, 88, 89, 96, 98, 99, 102, 103, 109 and 113 have been amended to correct clerical errors and to clarify the scope of the claims. None of these amendments are narrowing amendments or amendments made for reasons of patentability. Applicant respectfully requests favorable consideration and timely indication of allowance.

In the final Office action dated December 31, 2002, claim 54, 55 and 51 were rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg (U.S. 6,240,091) in view of Schneier. Claims 56-74 and 82-102 were rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg in view of Schneier as applied to claims 54, 55 and 81, and further in view of Walker (U.S. 6,263,438). Claims 75-80 and 103-116 were rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg in view of Schneier and Walker as applied to claim 54, and further in view of Thompson (U.S. 6,282,552). With respect to canceled claims 54-80, these rejections are moot. With respect to claims 81-116, Applicant respectfully traverses these rejections.

In response to the final Office action, Applicant submitted clarifying amendments and argued the merits of the case. The crux of Applicant's argument was that the claimed e-commerce system was a two-party system (i.e., the cardholder and the service provider). Through a mutual authentication process, the traditional third party certificate or authority could be eliminated. As part of the mutual authentication process, the service provider generated the session key for the transaction.

An advisory Action was issued by the Patent Office on June 20, 2003 refusing to enter the amendments and maintaining the rejections raised in the final Office action. The Patent Office took the position that the claims did not limit the system to a two-party system, indicating that a claim calling for a service provider that "exclusively" generates the session key would overcome the pending rejections.

In an interview with the Patent office on June 30, 2003, Applicant's attorney pointed out that each claim required that the session key be generated by the service provider. The Patent Office took a broader view of the claims arguing that a session key generated by the service provider does not prohibit third party participation. Although Applicant's do not necessarily agree with the Patent Office's interpretation of the claims, to expedite the prosecution of this case, the claims have been amended to expressly call for the generation of the session key "exclusively" by the service provider. This amendment is not a narrowing amendment made for reasons of patentability, but rather a clarification which merely states what was clearly implicit before.

In view of the foregoing amendments and remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance are respectfully requested. Should any issues remain which the Examiner believes could be resolved in a telephone interview, the Examiner is requested to telephone Applicant's undersigned attorney.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Craig Gelfound

Craig A. Gelfound
Registration No. 41,032

2049 Century Park East, 34th Floor
Los Angeles, CA 90067
(310)277-4110
Facsimile: (310)277-4730
Date: June 30, 2003

APPENDIX A

Claims 81, 84, 88, 89, 96, 98, 99, 102, 103, 109 and 113 have been amended as follows:

81. (Amended) A method of conducting an electronic transaction using an electronic card having a public key of a service provider, comprising:

formatting a key exchange request message at a member, at least a portion of the key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the key exchange request message from the member to the service provider;

generating a session key exclusively by [at] the service provider in response to the key exchange request message;

formatting a key exchange response message including the session key at the service provider;

sending the key exchange response message from the service provider to the member; and

using the session key to complete the transaction.

84. (Amended) The method of claim 82 or 83 wherein the use of [using] the session key to complete the transaction comprises:

formatting by the member a transaction request message using the session key, the transaction request message including a digital signature of the member, and sending the transaction request message to the service provider; and

formatting at the service provider, a transaction response message for the member using the session key, the transaction response including a digital signature of the service provider, and sending the transaction response message to the member.

88. (Amended) The method of claim 84 wherein the transaction request message comprises the response to the [a] service provider challenge.

89. (Amended) The method of claim 84 wherein the transaction response message includes data encrypted with the session key [a portion of the data].

96. (Amended) A method of conducting an electronic transaction using an electronic card having a public key of a service provider, comprising:

generating a member challenge by a [the] member;

encrypting by the member the member challenge using the service provider's public key from the electronic card to generate a first cryptogram;

formatting by the member a key exchange request message including the first cryptogram and a public key of the member;

signing digitally by the member the key exchange request message;

sending the digitally signed key exchange request message to the service provider;

generating by the service provider a service provider challenge;

generating exclusively by the service provider a session key;

encrypting by the service provider the service provider challenge and the session key using the member's public key to generate a second cryptogram;

formatting by the service provider a key exchange response message including the second cryptogram and a response to the member challenge;

signing digitally by the service provider the key exchange response message;

sending the digitally signed key exchange response message to the member;

encrypting by the member a member response for the service provider challenge using the session key to generate a third cryptogram;

attaching the third cryptogram to a transaction message going from the member to the service provider;

signing digitally by the member the transaction message going from the member to the service provider; and

sending the transaction message [going] from the member to the service provider [to the service provider].

98. (Amended) The method of claim 96 wherein the key exchange request message comprises the member's [cardholder's] public key encrypted with the service provider's public key.

99. (Amended) The method of claim 96 wherein the generation of the second cryptogram further comprises encrypting the member [a cardholder] challenge response as part of the second cryptogram.

102. (Amended) The method of claim 101 further comprising using the transaction identifier with a second transaction message following the transaction message and going from the member [cardholder location] to the service provider [location].

103. (Amended) A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the first key exchange request message from the first member to a second member;

combining at a second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider;

generating a first session key exclusively by the service provider in response to the first key exchange request message;

generating a second session key exclusively by the service provider in response to the second key exchange request message;

formatting a key exchange response message at the service provider including a first session key for the first member, signing the response message, formatting a key exchange response message including the [a] second session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member; and

separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.

109. (Amended) A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the first key exchange request message from the first member to at least one intermediate member coupled in series between the first member and the service provider, each of said at least one intermediate member being either a message router or a participating member;

generating, if said at least one intermediate member comprises at least one participating member, at each of the participating members a key exchange request;

receiving at the service provider a combined key exchange request message from said at least one intermediate member, the combined key exchange request message comprising the first key exchange request message and the key exchange request message generated by each of the participating members;

generating exclusively by [at] the service provider a first session key for the first member and a participating session key for each of the participating members;

formatting at the service provider a key exchange response message including each of the first and participating session keys;

sending the key exchange response message from the service provider to said at least one intermediate member;

separating by each participating member its respective participating session key from the key exchange response message; and

sending the first session key from said at least one intermediate member to the first member.

113. (Amended) A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a key exchange request message at each of a plurality of first members, the key exchange request message for one of the first members having a public key of said one of the first members, and at least a portion of the key exchange request message for said one of the first members being encrypted using the service provider's public key from the electronic card;

sending from each of the first members its respective key exchange request message to a second member, the second member being either a message router or a participating member;

generating, if the second member is a participating member, a second key exchange request message at the second member;

combining at the second member the key exchange request message from each of the first members to form a combined key exchange request message, the combined key exchange request message further comprising the second key exchange request message if the second member is a participating member;

receiving at the service provider the combined key exchange request message from the second member;

generating exclusively by [at] the service provider a first session key for each of the first members, and a second session key for the second member if the second member is a participating member;

formatting at the service provider a key exchange response message including each of the first and second session keys;

sending the key exchange response message from the service provider to the second member;

separating by the second member the second session key from the key exchange response message if the second member is a participating member;

separating by the second member the first session key for each of the first members from the key exchange response message; and

sending each of the first session keys to its respective first member.